Automatic Identification Technology (AIT)

Market Study

May 1995

Published by: Air Force Automatic Identification Technology (AIT)
Program Mangement Office

To obtain additional information,
contact the AF AIT PMO at the following:

AFMC-LSO/LOA
4375 Chidlaw Road, Suite 6
Wright-Patterson AFB Ohio 45433

DSN 787-4118 or (513) 257-4118 *voice*
DSN 986-1643 or (513) 476-1643 *fax*

Contents

Introduction

What is AIT?

Automatic Identification Technology (AIT) is a generic name given to devices used to automate data collection in a variety of applications, with the goal of providing cost savings by expediting the collection of accurate data. The AIT industries have been growing rapidly in the past five years, as both the DoD and commercial markets continue to identify uses for these devices. The primary AITs that DoD has been using are Linear Bar codes, Two Dimensional Bar codes, Radio Frequency (RF) Identification (RF/ID), Integrated Circuit Cards (ICCs), Memory Cards, and Laser Cards.

AIT Management in the Air Force

The AF AIT Program Management Office (PMO) is located at Wright-Patterson AFB in Ohio. It was established in 1994 by combining the AF Logistics Applications of Automated Marking and Reading Symbologies (LOGMARS) and the AF Microcircuit Technology in Logistics Applications (MITLA) PMOs. As part of DoD's continuing effort to streamline management, most of the services have combined their LOGMARS and MITLA PMOs into a single AIT PMO. The Air Force has followed suit. On a DoD level, these programs are managed by a Senior Advisory Group (SAG) consisting of Assistant Secretaries of the Air Force, Army, Navy, Marine Corps, DLA and GSA.

The AF AIT PMO manages all Air Force projects, and is responsible for managing every aspect of the AIT program in the Air Force. This includes continued development of DoD standards within the AIT arena, participating in various DoD AIT working groups, educating potential users regarding the capabilities of the technologies, cradle to grave project management, and the overall coordination, direction, development, and implementation of AIT within the Air Force. The AF AIT PMO personnel are all active project managers and are available to answer any questions you may have about the AIT program, as well as provide assistance to you in submitting your concept paper. The AF AIT PMO can be contacted as follows:

voice: DSN 787-4118 or (513) 257-4118
fax: DSN 986-1643 or (513) 476-1643

Why this Study?

As the focal point for AIT in the Air Force, the AF AIT PMO maintains up-to-date market data on a variety of AIT. This is done by attending conferences & standards groups, meeting with vendors, attending equipment demonstrations, and collecting product literature. This study is yet another way in which the AF AIT PMO stays in touch with state-of-the-art AIT, and provides this information to DoD customers.

Bar codes

Introduction

A bar code is an array of parallel narrow rectangular bars and spaces that represent a single character in a particular symbology. These bars and spaces are arranged in a particular order defined in the symbology. Bar codes are printed, scanned, decoded and then transferred to a host computer. This technology relieves the user of the tedious and error-prone task of having to read an alphanumeric label on an object and then transcribing the label contents onto a paper form or key-entering it into a database. Bar codes began finding their way into commercial markets in the early 70's, and the DoD has been using bar codes since the early 80's. MIL-STD 1189B is the governing standard for bar coding in the DoD. With bar code technology, the time required to identify objects and enter the identity code into a data base has been significantly reduced for many logistics-related operations at warehouses, retail stores, battlefields, hospitals, etc.

Symbologies

Linear Bar codes

Linear bar codes traditionally are used to represent a key data element that is used as a point of reference in a central database. Scanning the bar code provides for automatic access to the information in the database. Some of the more popular linear bar codes include: Universal Product Code (UPC), interleaved 2 of 5, code 3 of 9, and code 128. UPC is a fixed length numeric only symbology that was originally developed for the food industry to uniquely mark and identify products. The use of UPC has moved into other non-food retail applications. Interleave 2 of 5 is a variable length numeric symbology that is the standard Uniform Container Symbology (UCS).

In the Mid 80's, the DoD selected code 3 of 9 as the standard linear symbology. Code 3 of 9 is a variable length alphanumeric (set of 43 numeric, uppercase letters and some special characters) symbology. This symbology is in widespread use throughout the DoD, automotive industry and medical industry. Code 128, a relatively new linear symbology, is a variable length alphanumeric symbology with some advantages over code 3 of 9. Since code 128 offers higher coding densities, it is possible to print smaller bar codes with more data with code 128 versus code 3 of 9. Code 128 supports the full ASCII character set, and seems to be the focus of many industry and standards groups. While, the DoD continues to investigate the cost and merits of switching to code 128, code 3 of 9 is the only linear symbology approved for use within the DoD. Code 3 of 9 will remain the DoD bar code standard until the evaluation of other symbologies is complete.

Two Dimensional Bar codes

Two dimensional bar codes is a generic term usually used to refer to larger capacity bar codes. Some examples of two dimensional bar codes are Datamatrix, Code 1, Maxicode and PDF417. While a linear bar code can encode up to 17 characters, a two dimensional bar code can store 2,000 characters in a relatively small space (6 square inches). Two dimensional bar codes are also

Verification

A related topic to bar code printing is bar code verification. A bar code verifier is a small device that reads and analyses the bar code to determine whether the bar code is within the desired specifications. Verification should be a part of any bar code application.

Scanning

A scanner is a device used to read a bar code. It does this by projecting a beam of light onto the bar code. The dark bars absorb the light and the white spaces reflect the light back to the scanner. The scanner then converts the reflected light to a digital signal that is further decoded into the data represented by the bars and spaces. Types of scanners include wands, slot readers, hand-held moving-beam scanners, and Charge Couple Device (CCD) scanners.

Contact

The least expensive scanning device is the contact hand-held wand. This device is the size and shape of a large pencil. The operator places the tip of the wand just outside the bar code. With one continuous motion, the operator moves the wand across the bar code, and through the "quiet zone" following the symbology. Since the tip of the wand makes contact with the symbol as it moves across, scanning with a wand may damage the symbol itself. Another contact scanner is the swipe reader. The operator holds the bar coded document or card and moves (swipes) it through a slot in the reader past the reading beam. A swipe reader would be an excellent choice for reading the Code 3 of 9 on the back of the new Military ID Card.

Non-contact

Non-contact scanners do not require the operator to make physical contact with the bar code. Typically, the operator points the scanner at the bar code and pulls a trigger. The device then scans the bar code many times to achieve a complete read. This is a major advantage over the wand and slot scanners because with the wand or slot scanner the operator must create the scanning motion. If the first scan fails, the operator must repeat the scanning motion. Each scanning motion by the operator is considered one scan.

The hand-held laser scanner scans the bar code 40 to 100 times a second. This scanner employs a laser light source that is projected on to the bar code label and moved or rastered side to side through the symbol. A Charge Couple Device (CCD) scanner has a scan head comprised of light-sensitive diodes and light-emitting diodes. The user holds the scanner over the bar code to be scanned. The CCD-array senses the light reflected and absorbed from the symbol that is then decoded. A CCD scanner typically scans between 40 and 60 scans per second. This scanner is usually less expensive than a laser scanner, however, the scanner must be held very close to the bar code.

Scanners will continue to get smaller, increase in the number of scans per second, and become more intelligent. Most of the scanners today can read multiple symbologies.

Terminals

Bar code terminals are used to capture and/or transfer the scanned information to a computer. These terminals come in many different sizes, shapes and capabilities, however, they can be grouped into two categories: wedges and Portable Data Collection Devices.

Wedge

The most simplistic terminal is the wedge. The wedge is installed between the keyboard and display or CPU. It allows data to be scanned and sent directly to the application as if it was key entered. Some more sophisticated wedges can process information and store data.

Portable Data Collection Device (PDCD)

The second type of terminal, the PDCD may employ a small 2-16 line display, supplementary keyboard, memory storage capability, multiple communication ports, PCMCIA slots, full graphic displays, Radio Frequency Data Communications (RF/DC), Radio Frequency Identification (RF/ID) and smart card interfaces. Depending on the application, PDCDs can accommodate many variations on these options. Portable terminals are used when it is necessary to take the scanner to the asset, rather than bring the asset to a scanning station.

Radio Frequency Data Collection (RF/DC) combines the features of the PDCD and a two way radio to communicate real time data to and from a remote host. In applications that require a real time update to a database, this is an advantage over having to batch send data via a hardwire modem or a direct connect download. There are two types of RF/DC, narrow band and spread spectrum. Since each type has performance issues and regulatory restrictions associated with them, a Radio Frequency Specialist should be consulted before making an RF/DC decision.

The future for terminals is more features and interfaces to other devices and technology.

Bar code Vendors

ACC Systems, Inc.
AccuScan, Inc.
Action Systems Associates, Inc.
Advanced Industrial Systems
ALC Technologies PTE, Ltd.
Ann Arbor Computer
Application Consultants, Inc. (ACI)
ASA International, Ltd.
ASC Systems
Asset Management Technologies
AT&T, Network Systems Div.
Atlantic Bar Code Systems
Automated Solutions Corp.
Aztech America, Inc.
Badger Computers
Bar Code Solutions, Inc.
Bar Code Supply, Inc.
Bar Code Technologies
Bar Com
Barcode & Labeling Consultants, Inc.
BarCode Resources, Inc.
BMS, Inc.
C/Scan, Inc.
Cardinal Tracking, Inc.
Channel Technology Co., Ltd.
Clancy Systems International, Inc.
Columbia Labeling Machinery
CompuSpeak Laboratories, Inc.
Computer Identics Corp.
Computerwise, Inc.
Comspec Digital Products, Inc.
Comtec Information Systems, Inc.
Controlware Technologies Corp.
Corvallis MicroTechnology, Inc.
CyberNet Engineering
DAP Technologies Corp.
Data Automation Systems
Data Collection Products Co.
Data Collection Solutions, Inc.
Data General Corp.
Data Net Corp.
Data Tracker
DataDesigns
DataFlo Corp.
DataPort Technologies
Dauphin Technology, Inc.
DBK Concepts, Inc.
Digi-Matex, Inc.
Dovatron International
Dynasys
Epic Data, Inc.
Epson America, Inc.
Ergo Tech Corp.
Extech Instruments
Facility Management Systems, Inc.
Fascor
Foundation Resources
Fujitsu Personal Systems, Inc.
Furuno Electric Co., Ltd.
Gage Connections, Inc.
General Data Co., Inc.
Hand Held Products, Inc.
Handyer Technology, Inc.
Heartland Computers, Inc.
Husky Computers, Inc.
1-0 Solutions, Inc.
IBM Corp., Altium Co. Div.
ICC, Inc.
ICIS, Inc.
ICS International AG Identcode
Systems
InData Systems
Indiana Cash Drawer Co.
Industrial Auto ID, Ltd.
Inforite Corp.
Informix ID Systems
Infoscan, Inc.
Innovative Products & Peripherals
Integrated Barcode Solutions
Integrated Barcoding Systems
Intermec Corp.
ITP Business Communications
Jacobsen Holz Corp.
Jet Equipment Corp.
Jetech Data Systems, Inc.
K-Ram Corp.
Kassoy Automated Solutions (KAS)
Kearney Systems, Inc.
Laserlight Systems, Inc.
Laftice, Inc.
LXE, Inc.
MacKechnie Consulting Group, Inc.
MacSema, Inc.
Management Technology
International, Inc. (MTI)
Manufacturing Systems Associates
Marketing Associates
Mars Electronics
MCD Corp.
Micro Palm Computers, Inc.
MicroRidge Systems, Inc.
Millstone Sales and Service Corp.
Mitron Systems Corp.
Moffom Data Collection
National Datacomputer, Inc.
National Technology Services, Inc.
Neuron Electronics, Inc.
NFS Radiation Protection Systems
Nimax, Inc.
Norand Corp.
Ohm Systems, Inc.
Omnicode Data Systems
Omnidata International, Inc.
Opticon Sensors Europe B.V.
Panasonic Communications &
Systems Co.
Par Microsystems Corp.
Paradise Barxon Corp.
Peak Technologies Group, The
Pearl Worldwide Industries, Inc.
Penflex Elektronik GmbH
Precision Resource Corp.
Process Control Systems, Inc.
Productivity Enhancement Products
Progressive Microtechnology, Inc.
Psion, Inc.
QED Information Systems
Qualtec S.A. de C.V.
Radix Corp.
Recognition Equipment Brokers, Inc.
Ryzex Re-Marketing
Samco Time Recorders, Inc.
ScanSource
Scanco
Second City Software
ShopTrac Data Collection Systems
Simple Solutions, Inc.
Skandata Corp.
Software Integration Services, Ltd.
Somerset Automation, Inc.
Southern Micro Systems, Inc.
Standard Register Co., The
SunDisk Corp.
Symbol Technologies, Inc.
Systel International SpA
System Concepts
Telxon Corp.
Time Tech, Inc.
Tom Zcsel Associates
Tren Tech, Inc.
Tridata Technologies, Inc.
United States Data Corp.
Universal Data, Inc.
Verbex Voice Systems, Inc.
Veritec, Inc.
Videx, Inc.
William Miles Associates, Inc.
XEC Computer Products, Inc.

Integrated Circuit Cards
"Smart Cards"

What is a smart card?

An integrated circuit card, more commonly referred to as a smart card, is a device the size and shape of a credit card and contains an electronic chip allowing it to process as well as store information. Smart cards can contain read-only memory (ROM), read/write memory, or a combination of both. A reader can access the chip either through direct physical contact with the chip, or via an inductive coupling technique.

These devices are most likely to be used for pre-paid financial transactions (e.g., vending machines, pay phones, rented cellular phones, public transit, etc.), personal information database activities (e.g., medical history information), or as identification devices to be used for access to highly secure facilities or computer networks. Smart cards have become very popular in Europe and parts of Asia, and are beginning to become more widely embraced in the US.

How are they used?

Electronic Purse

Numerous currencies are used throughout the European continent. If a French traveler in Germany wants to use a vending machine or pay telephone, he or she must have the appropriate coinage to make the purchase or place the call. On the other hand, if he or she were to have a smart card containing a pre-paid currency, then the vending machine or telephone could debit the cash from the card using the most recent value for the currency exchange. Everyone is happy. The vending machine company gets business which it might otherwise miss, and the traveler has the convenience of not having to change currency and carry all of the various types of coinage. Furthermore, the vending machine company or telephone operator does not have to send someone to collect money from the coin box. Though having the right color of money is not an issue in the US, debit cards are becoming more popular as they reduce the need to carry cash, and reduce theft from the vending device. Smart cards are becoming especially popular on college campuses where students can use their debit card to do their laundry, make copies, buy snacks, etc. Since this same card can have a photograph placed on it, the card can also be used as their campus ID card.

Off-line verification

Credit card transactions in the US are generally made by transmitting a card identification number and transaction amount to a central data base for on-line confirmation. The card is authenticated and validated in near-real-time. The authentication process ensures that the card was properly issued, and the validation process confirms the owner's name and ensures that the card has not been stolen or the credit limit exceeded. All of this happens quickly while the customer waits. In Europe and other parts of the world, remotely accessible central data bases are not nearly as well developed as they are in the US. Therefore, these locations require that each transaction be verified at the point of sale. The authenticity and validity checks must be made using only information available on the card. In these cases the point of sale operator must ensure that the card was authentically issued, that the card-holder is in fact the legitimate owner, and that the card is still valid for use.

Smart cards provide a consistently secure method of performing this check, as the microprocessor in the chip can be used to do the processing thereby eliminating the need to telephonically connect to a data base. Access to the chip can be protected by a Personal Identification Number (PIN) so that simply having the card does not mean the account can be charged. This is similar to an Automated Teller Machine (ATM) transaction whereby you must enter the correct PIN in order to use the card and access the bank account. The chip can be configured so that if the PIN is incorrectly entered three times, the card is rendered useless. This is also similar to the ATM configuration whereby the ATM keeps the card after three failed attempts to access the card. One of the differences between the two cards is that use of the magnetic stripe on the ATM machine requires that the ATM reader be able to communicate back to a central data base. Since the smart card contains a microprocessor, once the card is inserted into a reader/writer device the card itself can process the transaction. There is no need to connect to another computer to complete the transaction.

Security

Magnetic stripe cards can perform some of the functions described above, however, they can be easily compromised. They are not difficult to forge or to manipulate so as to gain unauthorized access to the information contained on the stripe. Even if a PIN number is stored on the magnetic stripe, a card thief can decode the PIN and use it with the card to successfully complete a transaction. The system has no indication that the card was invalidly used. Additionally, if the magnetic stripe contained a stored currency value, even a legitimate card holder could illegally increàse the value in the card by using commonly available equipment. With a smart card, all information stored on the card can be protected against unauthorized access. Such cards offer a very high level of security to the card issuer, the point of sale merchant, and the owner of the card.

Given the above discussion, it is understandable why smart cards have first found greater acceptance outside of the US. However, it is likely that their use will grow in the US in areas of small pre-paid financial transactions where central data base transactions are either too expensive or too time consuming. In addition, closed loop institutions such as universities are finding that many functions from financial transactions to access control can be accomplished with appropriately designed smart cards. The tables on the following pages list those companies which manufacture and sell smart cards and smart card terminals throughout the world.

Smart Card and/or Terminal Manufacturers

Company	Headquarters	Comments
Angewandte Digital Elektronik GMbH	Germany	Contactless cards only with a specialty in automotive keys using inductive RFID; encryption capability.
Algorithmic Research Ltd.	Israel	RSA smart card (no memory capability listed)
AT&T Smart Card	New Jersey	Up to 8K bytes of EEPROM in a contactless card. ISO Part 1 and 2 and ISO financial transaction compatible; Security includes DES algorithm, MAC, and bilateral authentication.
Bull CP8	France	Up to 8K bytes EEPROM contact cards with DES algorithm, bilateral authentication, T=0 and T=1 protocol; multi-user and multi-service cards with very high speed data rate (up to 115,000 baud); cards used in more than 200 food stores in Dayton for food stamp program. Terminals include "dumb" ones that connect to PC and smart stand-alone systems with display and key pad; the company also makes network security software for access to computer networks.
Buscom Oy	Finland	Largest smart card manufacturer in Finland; all RFID proximity cards used for bus fare collection.
Dai Nippon	Japan	CPU-based cards with EEPROM up to 32K bytes; also manufactures IC/optical card hybrid; also manufactures photo ID cards with direct printing.
Data Card	Minnesota	16 bit CPU cards with up to 8K bytes EEPROM and 10K bytes ROM; special embossing, card personalization; large field service organization. Manufactures programmable POS terminals as well as workstation-networked terminals with modem for on-line transactions.
Debitek	Tennessee	Joint venture with Girovend in the U.K.; largest cashless payment company for vending machine operations.
dz Danmark	Denmark	plastic card and smart card manufacturer
Gemplus	France	Manufacture 13 million cards/month; ISO 7816 Parts 1 & 2 compatible; cards with up to 8K bytes EEPROM with up to 255 independent files with a combination of up to 15 secret codes.
Giesecke and Devrient GmbH	Germany	8K byte EEPROM cards with 8 bit microprocessor; significant player in the German Health Insurance Program; Stand-alone terminals, programmable, displays, keypads, cryptographic algorithms.
Girovend	U.K.	World's largest manufacturer of vending machines using smart cards; 2K bytes of EEPROM in a contactless card.
GPT Card Technology	U.K.	Contactless memory cards with an 8 bit micro-controller with security functions. 2 million card/month capacity; major player in pre-paid phone cards.
IBM (UK) Ltd	U.K.	Multi-function card with up to 8K bytes EEPROM, DES algorithm, authentication capability, PIN checking algorithm

Intellect Australia	Australia	Super smart card with 16 key keypad, audio beeper, 16 character LED display, battery. DES algorithm and cryptographic processing. Smart card read/write capability with built-in modem and phone number storage; also a PIN pad.
Landis and Gyr Smart	France	Major applications are pre-paid electric and natural gas metering; physical and logical access control. Multi-purpose read/write terminal with networking link options.
McCorquodale Card Technology Ltd	U.K.	Major strength is plastic card manufacturing
Matsushita Battery Industrial Company	Japan	8 bit micro processor with EEPROM capacity up to 8 K bytes
Mikron	Austria	Fastest multi-function/multi-application single chip processor card -- 153,000 baud, contactless inductive card, ISO 7816 Part 3 T=1 protocol.
Mitsubishi Electric UK Ltd	U.K.	Contactless card, 8 bit micro processor; data rate: 153,000 baud
Orga Kartensysteme GmbH	Germany	Stand-alone and PC-connected read/write terminals; also simulation product for evaluating GSM handset systems.
Personal Computer Card Corp	Florida	DES and RSA smart cards for physical and logical access control, electronic benefits transfer programs, etc.
Philips TRT Smart Cards and Systems	France	5 million card/month manufacturing capability; logical and physical access control, telecom, GSM mobile telephone. Numerous terminal models- stand-alone and PC-embedded complying with T=O and T=1 communication protocols.
Racom Systems, Inc.	Colorado	Inductive RFID proximity cards with up to 500 bytes of ferro-electric RAM (FRAM)
Schlumberger Smart Cards and Systems	France	More than 200 million cards produced to date; cards in use in over 60 countries. They offer a complete line of smart card terminals, including fixed, handheld, and cordless as well as being the largest manufacturer of smart card pay phones in the world.
SDU Chipcard Technology	Netherlands	Largest smart card manufacturer in the Netherlands; many applications including an RFID toll collection project with Amtech.
Setec Oy	Finland	8 bit CPU with EEPROM up to 3 Kbytes, DES encryption
Siemens Nixdorf Informationssysteme	Germany	ISO compatible, T=1 protocol, 8 bit microprocessor.
Solaic Smart Cards	France	Up to Kbytes EEPROM in microprocessor card
Tactel Ltd	Israel	Contactless cards with proprietary authentication capability and PIN protocol.
Toppan Printing Co. Ltd	Japan	Contact and contactless with up to 32K bytes EEPROM with DES encryption and using T=1 communication protocol.
US3	California	Largest US manufacturer of smart cards with a 4 million card/month manufacturing capability;
Veron SpA	Italy	Up to 8K bytes EEPROM microprocessor cards.
Auscom Autelca AG	Switzerland	Major application area is smart card ticket vending machines; also makes pay phone terminals accepting coins, magnetic stripe, smart card, watermark magnetics cards.

AT&T Global Information Solutions Ltd	Scotland	Manufactures more than 40% of the world's ATM machines which use smart cards, magnetic stripes, biometrics, etc.
COGITO Technologies	France	Multiple services smart card terminal for access control, electronic payment, etc.
Dassault Automatismes et Telecommunications	France	Manufactures portable smart card terminals for taxis, airports, and fixed multi-service and ATM terminals.
De La Rue Fortronic Ltd.	Scotland	Full range of fixed and portable smart card terminals for off-line and on-line transactions with displays.
HTEC	U.K.	Smart card read/write terminals with interface to PC and also stand-alone ISO smart card terminals.
Innovatron	France	Major market applications in smart card parking meters and also experimental markets involving electricity, gas, and water metering.
Inter Marketing Ltd	Finland	Manufactures portable and fixed terminals for both contact and contactless smart cards; Major application is in public transit where end-of-day fare collection data is sent to central computer via RF modem.
InterCard GmbH Kartensysteme	Germany	Major player in smart card terminals for cashless payment for photocopying machines; Multiple language capability and menu driven displays.
ITC Systems	Ontario, Canada	Manufactures a range of embeddable smart card readers/controllers for cashless machine payment and control
Micro Card Technologies Inc.	Virginia	Subsidiary of Bull CP8 (See Bull for products)
Monetel SA	France	Largest manufacturer of smart card pay phones
NET 1 Products Ltd	South Africa	Various PIN pad, smart card readers and terminals
Oki Electric Europe	Germany	No information
PT Bauma Smarti Teknika	Indonesia	Smart card transaction terminals
Racal Datacom Ltd	U.K.	Smart card terminals with PIN pads for cryptographic computer access control.
Sec-Com	Czech Republic	Smart Card terminals at gas stations
Software House Riga	Latvia	Smart card terminals for account systems and computer access control.
Telesincro SA	Spain	Smart Card Verification Terminals with fingerprint biometric capability embedded; also portable smart card reader.
Thyron Ltd.	UK	Fixed and handheld smart card terminals for financial transactions and computer security.
Veri Fone Inc.	California	Fully networked smart POS terminals with displays and programmable function keys
Wayfarer Transit Systems Ltd	UK	Smart card terminals for transit ticketing; will accept contact and contactless cards
Wellcom GmbH	Germany	Smart card and magnetic stripe terminals for use in taxicabs
Westinghouse Cubic Ltd.	UK	Fare collection systems using contactless smart cards; include complete systems integration capability.

Personal Computer Memory Cards

Background

Personal computer memory cards are beginning to become an important part of the digital storage device marketplace. The importance of these devices has grown proportionately with the increase in popularity of small portable computing devices such as sub-notebook and palm-sized computers. As these battery driven devices proliferate, the need to have smaller, more rugged, lower power memory devices has escalated. The development of small credit card sized storage devices, which can be interchangeably inserted into portable computing devices, allows the portable devices to carry a considerable amount of stored data or application software. Memory cards can come in a variety of silicon types, ROM, EPROM, EEPROM, Flash memory, etc. The choice depends upon whether the requirement is for read-only or read/write memory, the amount of memory required, cost, etc. Each type of card is optimized for a particular application, such as storing programs or large variable data bases.

Probably the fastest growing type of silicon device used in memory cards is flash memory, which unlike RAM does not need to have a continuous power supply to maintain the integrity of the stored data. This type of memory is generically known as "non-volatile" memory. Flash memory has been optimized both in terms of its ability to use low power for erasure and re-write operations, as well as its ability to pack a large amount of memory capacity into a small space. All of these solid state storage cards are not only competing with each other in the portable computing market, but also with miniaturized hard disc drives. The key factors involved in the process of selecting a type of large scale memory system for portable devices are: size, energy use, memory capacity, ruggedness, cost, and the availability of industry standards.

Size

Size is the key factor driving the industry, because the basic computing devices are becoming increasingly smaller in order to meet consumers' demands for smaller, more conveniently portable devices. The Personal Computer Memory Card Industry Association (PCMCIA) has established standards for three sizes of cards. These are known as Types I, II, and III, all of which have the same length and width dimensions (approximately a credit card size) and range in thickness from about 1.5 mm to 10.5 mm. Computer vendors are increasingly offering PCMCIA slots in their machines, especially for the very small laptops and palmtops. Where such slots are not built directly into the machines, external card readers may be used as an external peripheral device with a port connection into the computer.

Energy Use

Hard disc drives use considerably more energy than most solid state devices. Energy usage is especially important when a battery driven portable computer is being used. Battery capacity and weight are key issues in the portability and usefulness of any portable device. The use of low power silicon-based memory systems provides considerably more computer usage time between re-charges than does a continuously spinning hard disc.

Memory Capacity

Memory capacities for these cards vary from about 250 Kbytes to 64 Mbytes. Small hard disc drives can contain memory capacity exceeding 100 Mbytes. The memory card capacities will continue to increase as semiconductor manufacturers move to smaller and smaller "feature" sizes, but hard drives will probably continue to be able to maintain a lead in terms of the memory density of the discs as compared to solid state memories.

Ruggedness

Ruggedness is a major consideration for very small computers, such as palmtops, because they are carried around in unprotected environments (in regard to shock and vibration). Hard drives generally are neither very shock or vibration resistant, and furthermore they may not be able to be successfully used while being held in non-traditional positions. Generally speaking, positions other than the traditional horizontal position may adversely affect the spinning motion of a disc. This is not a problem for solid state memory devices, and it is therefore an area where solid state devices have very distinct advantages relative to hard disc drives.

Cost

Memory card costs are currently still in excess of $10/megabyte which puts them at a distinct disadvantage to miniature hard drives. However, if a palmtop computing capability is essential, then the cost issue will probably not be a significant barrier to the use of memory cards.

Standards

In addition to the card size standard, the PCMCIA is also establishing standards for the physical interconnections and power supplies. This will ensure that any card can be inserted into any PCMCIA standard slot. Most computer operating systems generally have a driver for accessing memory from a hard drive, however, those drivers may not be compatible with the access mode for a memory card. This incompatibility currently requires the host to have a driver for each specific type of memory card to be used, or requires the card to have a resident operating system. This latter approach is costly both in terms of wasted storage capacity on the card, as well as in the time required for the computer to access the card's operating system. The industry is addressing this concern for a standard memory card access driver, and in fact Intel has developed a chip set which will allow many different types of cards to be interchangeably used in any computer. Intel calls its system the Intel Exchangeable Card Architecture.

Vendors

A listing of memory card vendors is provided on the following page.

Memory Card Vendors

Company	DRAM	SRAM	PSRAM	OTPROM	MROM	Flash	EPROM	EEPROM
50/50 Micro	X	X				X		
Advanced Micro Dev.						X		
AMI Semiconductors	X	X		X	X	X		
AMP		X				X		
Atmel						X		
Berg Electronics	X	X	X	X	X	X	X	X
C-ONE Technology	X	X	X	X	X	X		
Camintonn Corp.	X	X						
Cardwell International		X		X	X	X		
Catalyst Semiconductor						X		
Celestica	X	X				X		
Centennial	X	X		X	X	X		
Century Microelectr	X	X						
Chaplet Peripherals		X				X		
CIM Engineering, Inc.	X	X				X		
Cubic Memory	X							
Dallas Semiconductor	X	X						
Data 1 Inc.	X	X				X		
Datakey		X		X				X
Enhance Memory	X	X						
Epson America	X	X	X	X	X	X	X	X
Exel Microelectronics		X						
EXP Computer, Inc.	X	X				X	X	
FDK America Inc.	X	X	X	X	X	X		
FujiFilm Microdevices	X					X		
Fuijitsu Microelectr.	X	X	X	X	X	X	X	
Hitachi America, Ltd.	X	X		X	X	X	X	X
IBM	X	X		X	X	X		
Intel						X		
Kelly Microsystems	X							
M-Systems								
Magic RAM	X	X		X		X		
Matsushita	X	X	X	X	X	X	X	X
Maxell Corp.	X	X			X	X		
Maxtor						X		
Micron Semiconductor	X							
Mitsubishi	X	X		X	X	X		X
Motorola	X							
MultiTech Systems	X	X				X		
NEC						X		
New Media Corp.	X	X		X	X	X		
OKI Semiconductor	X	X						
PreMax		X			X	X	X	X
Pretec Electronics	X	X		X	X	X		X
Psion PLC		X		X		X		
Quantum								
Rohm Corp.	X	X		X	X	X		
Samsung Semiconductor	X	X			X	X		
SCM Microsystems	X	X		X		X		
SGS-Thomson	X							
Sharp Electronics		X		X	X	X		
Shigma/Fujisoku	X	X		X	X	X	X	
Silicon Storage Tech.						X		
Simple Technology	X	X				X	X	
Smart Modular Tech.	X	X	X	X	X	X		X
Sundisk Corp.						X		
Texas Instruments	X			X		X		
TLCI, Inc.	X	X		X		X	X	
Toshiba America	X	X			X	X		
Transcend	X	X			X	X		
Verbatim		X				X		

Optical Memory Cards
"Laser Cards"

Background

Laser card technology is relatively new and is very similar to the now familiar audio CD and audio-visual CD-ROM. The primary difference is the form factor. The laser card has a form factor which is roughly similarly in size to a credit card. This makes it easily carried by a person in a pocket or wallet. Though all of the optical technologies are essentially write-once/read-many times (WORM), the laser card differs in that information is written to the card in increments rather than having all of the information loaded at one time. The laser card can have data written to it in a sequential order on many occasions until all of the available memory has been used up.

Laser card technology works on the principle of reflectivity. Data is written to the card with a narrowly focused high intensity light beam (e.g., a laser). This light source is used to burn a small hole in the surface coating of the card. The newly exposed sub-surface coating (known as a pit) has a lower reflectivity than the surface coating. The reflectance differences of the surface and the sub-surface round pits are used to define a "0" or a "1" bit, i.e. low reflectance will be interpreted as "0" and high reflectance will be interpreted as a "1" bit. When data is written to the card, one type of light source is used to create the pit pattern. This pattern is subsequently able to be read by a different light source by scanning it and obtaining a reflectance pattern, which is interpreted as a string of digital bits. As with any digital machine, the bit string is then converted to useful alphanumeric information.

Characteristics of the Technology

<u>**Advantages**</u>

- A very large amount of memory is available for a relatively low price. Up to 4 megabytes of memory may be contained on a single card costing only a few dollars.

- All of the memory is non-volatile, i.e. it is protected memory which is not dependent upon having an electrical power supply to maintain it.

- The laser cards are very rugged. They are more flexible than smart cards; more rugged if hit or moistened, and cannot have the memory damaged in the presence of high magnetic fields, as can be the case with magnetic disc or tape memory.

Disadvantages

- The reader equipment is expensive, bulky (i.e., it is not available in a handheld device), and requires the use of a PC in conjunction with the reader.
- The data transfer to and from the card is relatively slow as compared with silicon or magnetic disc memory.
- Access to the memory is not as secure as with smart cards
- The card must be discarded once all of the available surface area on the card has been used up with burned-in pits.

Applications

The applications for the laser card involve those for which a large amount of information needs to be carried around in a compact, rugged device. Such applications include:

manifest information for shipping pallets and containers

medical and dental records for an individual (including x-ray images)

maintenance manual information

map and terrain information

Biometric identification information including photograph, fingerprint, voice print, etc.

financial account information

Vendors

Many of the vendors of laser cards and reader systems manufacture under license to Drexler Technology Corporation of Mountain View, California, which holds the basic patent on the use of laser read/write systems. Included in this group is Laser Card Systems, a Drexler subsidiary, and a number of Japanese companies including: Canon, Dai Nippon, Optical, Olympus, Omron, and Nippon Conlux. Another company with a patent position for larger memory cards is Optical Recording Corporation of Toronto, Canada.

Radio Frequency Identification
RFID

Technology and Method of Operation

RFID is a relatively new approach to automatically identifying, categorizing, and locating people and assets over relatively short distances (a few inches to hundreds of feet). The RFID labels are known as tags or transponders. They contain varying amounts of information ranging from an invariant ID number programmed into the tag at the factory to a 128K byte variable memory which can be programmed by a controller unit using RF radiation. The controller unit is usually referred to as a reader or an interrogator.

RFID interrogators communicate with tags through the use of radio frequency (RF) energy. The interrogator sends out an RF signal which "wakes up" the tag, and the tag transmitts information back to the interrogator via RF. In addition to reading the tag, the interrogator uses RF energy to write new information to the tag. This enables the user to alter the information stored in the tag from a distance. Interrogators can be networked together so as to provide nearly unlimited coverage for a system.

Applications

The potential applications for this technology are numerous. RFID technology offers inexpensive read-only tags, which are generally short range (a few inches to a few feet), or more expensive long range, read/write devices with large memory capacities. The short range tags can be used in lieu of bar codes for identifying objects in harsh environments. For example, these tags are used in factories to track items through their production cycle. Given the short read range of these tags, the item typically travels on a conveyor bringing it in close proximity to the interrogator. Short range systems are also used for personal identification and access control operations. The identity of the individual can be determined either with a very short range RFID card read when held within a few inches of the reader, or with somewhat more expensive systems which can read the card even when it is kept in a pocket.

The longer range tags are finding many applications in transportation, as these tags can be read at distances up to several hundred feet. They are being used to identify vehicles on roadways, as well as for automatic toll collection. Once the vehicle's account number is read by the interrogator, a debit is made to the vehicle owner's account, which may be located in a secure central data base or in the tag itself. Additionally, rail cars are being tagged so that the railroads will have real-time location data of their rail cars. Trucking companies and intermodal container carriers are using these systems to identify their vehicles (and in some instances their contents) electronically as the tagged containers move past interrogators in ports or truck terminals.

These longer range tag systems are also capable of being used in depots, factories, and warehouses to provide automated inventory of assets with no human involvement. In addition to automatically identifying the assets, these systems can locate the assets and direct a person to the asset very quickly. There are many other potential uses for this technology both in military and commercial applications, especially as the cost of the systems continue to decrease.

Cost

The small short range tags can be smaller than a fingernail and cost $1- $20. The longer range *read-only* backscatter devices generally cost $10-$30, while the *read/write* backscatter versions cost $30-$75. Active read/write tags (battery required) cost $55-$200 depending on features and size of memory. All of these costs are moving down, however the cost reductions for active tags may not be as dramatic as with backscatter tags due to the requirement for a battery in an active tag.

The cost for an interrogator unit varies from $500 for a very short range tag interrogator to $2000 for an active tag interrogator, and up to $8000 for a backscatter interrogator. Vendors also offer fixed and handheld interrogators and some specialized software for their equipment.

Standards and Regulations

The Federal Communications Commission regulates the use of all RF transmitting devices in the US. Similar agencies perform that function in other countries. In the US and other countries, transmitting devices can either require licenses to operate in specific locations at given frequencies and power levels, or they may be granted a blanket certification to operate anywhere if they operate in an allowable frequency band and remain below certain transmitted power levels. The allowable frequency bands for the latter type of operation are proscribed by the FCC. Backscatter interrogators typically require licenses while the short range and the active interrogators can be certified to operate without licenses.

As of the preparation time of this document, there is one ANSI/ISO standard for RFID tags. It is for use with intermodal containers. Other standards include a mandatory standard from the American Association of Railroads and a voluntary standard from the American Trucking Association. There are two other national standards in some stage of development, i.e. a standard for Automatic Vehicle Identification (AVI) being developed by ASTM and a generic active RFID tag standard being developed by the X3T6 Committee of ANSI. Finally, the State of California has published a standard which is to be used for AVI applications within the state. The State of Kansas has required the California standard be used in its automatic toll collection on the Kansas Turnpike.

RFID Companies

Company (Type of Product)	Line of sight required?	Read/Write?	Memory Size	Range	Multiple Tag Read Capability?	Frequency	FCC Site License Required?	Time to Download 128 Kbytes	Handheld Interrogator Available?
ASGI (Passive, active tag under development)	Yes	Yes	115 bytes	<2.5 meters	Yes	66/132 KHz	No	Not applicable	No
AT/Comm (Active)	No	Yes	10 Kbytes	>2000 feet	Yes	2.45 and 5.8 GHz	Yes	<30 minutes	Yes
ID Systems (Active tag under development))	No	Yes	64 Kbytes	50 meters	Yes	UHF, 915 MHz, and 2.54 GHz	No	2 minutes	Yes
Intellitag (Passive, and active)	No*	Yes	2 Mbytes	>10 meters **	Yes	915 MHz and 2.54 GHz	yes ***	<4 seconds	In development for active tag
Rand Technologies (Active)	No	Yes	128 Kbytes	150 meters	Yes	903-928 MHz	No	< 2 minutes	In development
Saab Scania Combitech (Passive)	No*	Yes	8 Kbytes	> 10 meters	Yes	2.45 and 5.8 GHz	No	<5 seconds	Yes
Savi Technology (Active)	No	Yes	128 Kbytes	150 meters	Yes	315 or 433 MHz	No	< 28 minutes ****	Yes
Single Chip Solutions (Passive)	Yes	Yes	1 Kbyte	<2 meters	Yes	125 KHz	No	Not applicable	Yes
Texas Instruments (Passive)	No	Yes	512 bits	<2 meters	No	120 KHz	No	Not applicable	Made by other companies
XCI (Passive)	Yes	No	26 bits	10 meters	Not in the current products	915 MHz	No	Not applicable	In development

* Range is reduced if line-of-sight situation does not exist.

** The active version with the same protocol has a range of about 150 meters.

*** The active version will not require a site license.

**** Capability exists to intelligently search for data. Direct connect downloads < 1 minute.

Definitions of RFID Terms

Passive and Active. RF tags communicate with the interrogation units via radio frequency radiation. The electrical power to drive the tag's communication capability can either be derived from the incident radiation arriving from the interrogation unit or by an electrical supply source (e.g., a battery) located on the tag. Tags which derive their transmitting power from the radiation impinging on the tag are known as passive devices. They either use the magnetic field from the interrogator's signal or the electric field. If they use the former, then they are known as inductive tags, which use low frequency RF radiation and have very short communication distances. When the electric field is used to power up the tag, these devices are referred to as backscatter or reflective tags and usually utilize higher frequencies and achieve longer communication distances. When the tag has its own power source for transmission, those tags are referred to as active tags and can usually achieve even longer distance communication.

Range. The effective maximum distance over which the tag and interrogator can successfully communicate.

Line-of-Sight In order for any communication to occur, a signal transmitted from interrogator or the tag must reach the other device. Unless the device is in a completely shielded metal enclosure, some radiation will usually reach the device. This radiation may arrive in a direct line of sight path or it may arrive via scattered reflections from man-made or natural terrain features. However, the amount of radiation (and its phase) which reaches the device is very important. If a passive device is being used, sufficient radiation must reach a tag so that the tag can not only can interpret the information content of the signal, but must also be sufficient to power the signal transmission of the tag back to the interrogator. Therefore, passive devices usually have a significant degradation in their range when they are not in the direct line of sight to the interrogator, because otherwise they will not receive enough RF radiation to allow for a successful re-transmission of RF radiation. Active tags are much more non-line-of-sight tolerant, because they only need to receive enough radiation to allow for the incoming signal to be successfully interpreted. They then re-transmit using their own on-board power supply.

Read/Write Capability. Some RF tag systems only allow for data to be encoded once in the tag's memory. This encoding may be performed in the factory or by the use of special equipment in the field. Those tags are referred to as read-only devices. Tags, whose memory may have data written to them remotely and repeatedly via RF signals are referred to as read/write devices

Multiple Tag Read Capability. In some instances it is necessary to identify all tags in a given area. This can always be accomplished if one tag at a time is placed in the RF field of the interrogator. However, if the tags are randomly spread out over an area, it is desirable for the interrogator to transmit a command over the entire area (this is known as an omni-directional signal transmission) requesting the identity of all tags. If all tags were to simultaneously respond to that command then the various RF signals would interfere with each other and the interrogator would receive only RF noise. Many systems have been developed which allow the tags to be individually "heard" by the interrogator thus avoiding the RF chaos of many interfering signals.

This multiple tag reading capability is usually achieved by randomizing the response of each tag into different time slots or having each tag respond at a slightly different non-interfering frequency.

Data Rate. The speed at which data can be read from or written to the tag via a radio link. This is usually expressed in bits or bytes per second or baud, which is bits per second. Because most systems will have time delays due to error checking and moving data around the internal memory of the tag, the full data rate is not actually achieved in practice. Furthermore, in some cases, there will be further limits on the data rate imposed by the requirements of the Federal Communications Commission (FCC) or other similar regulatory bodies in countries outside the US. Therefore, the relevant value used in the survey table is the amount of time which is required to move 128K bytes of data into or out of the tag memory. In some cases, companies do not show the capability for 128K bytes of memory in their current product line, so they were asked to compute the time for a 128K byte transfer if their product had that much memory.

FCC Licensing. In the US all devices which emit RF radiation are regulated by the FCC to avoid radio chaos from interfering signals. The FCC can either provide a vendor of transmitting systems with a license to transmit at a given site using a given frequency and a maximum transmission power level, or it can provide a certification that at a given frequency the power levels are so low as to not pose a major interference threat. When a company's products are regulated in the latter manner they are said to require no license and are certified under the FCC's Part 15 Rule for unlicensed certification. This is important, because one might want to use tags and interrogators in a variety of locations and not need to go through the license application process for each individual location where the system is to be used.

VOICE-Based Data Collection
Speech Recognition

The Technology

Speech recognition is a relatively new technology. It can be used to enter data into a computer or other digital storage device using the spoken word, which allows the individual entering the data to do so with his/her hands free. The technology operates as follows:

- The sound pattern (i.e., the frequency/intensity spectrum over time) of a spoken word is digitized and stored in a computerized "look up" table.
- The digitally stored words comprise the vocabulary "template" in the computer.
- When a user speaks into the microphone during a speech recognition activity, the sound pattern is similarly digitized and compared against the words already digitally stored in the template.
- If a match is made, the matched word is sent in its proper sequence to either a computer memory, a visual display, or a printer device.
- The appropriately sequenced words can then be used to generate a complete report of an inventory inspection, a loaded truck manifest, etc.

There is a limit on how many words can be stored in memory because each word in the template uses about 3,000 bytes. Furthermore, the more words stored in the memory, the longer it takes to do the comparisons of the real-time spoken word relative to the stored words in the template in order to find a match. In other words, such systems are constrained by available memory and processor speed. In addition, the systems are usually limited to the words spoken by specific individuals. Therefore, if three people were to use one portable unit, even if the same words were stored in the computer, there would probably have to be a different stored template for each user.

A typical portable speech recognition system ususally consists of a belt-worn unit containing the stored template, as well as the sound processing unit. A separate battery pack would probably also be worn on the belt. A headset with earphones and a microphone (wired to the belt-worn unit) would also be provided. The portable unit worn on the belt would be able to have its input downloaded to a remote computer in real-time via a radio link, or it could be downloaded at the end of a shift using a hard wire link, such as an RS-232 connection. Once in the computer, the downloaded input could be displayed, processed, or printed in a hard copy report format.

Applications

A typical application might be a safety audit. An inspector would be prompted by questions posed by the portable unit and received audibly by the user, who would then respond to the question with one of the stored template words. A typical question might be: "What is the maintenance status of the landing gear?" The inspector would look at the landing gear and respond saying "the number six bolt is loose." If all of the words in quotes were stored in the template, then the matched text would be stored in the belt-worn unit as the answer to the question. The answer could also be transmitted in real-time by a wireless link to a local computer which could display, store, or print out the question and the answer. An entire inspection could occur in this manner. This allows the inspector to have his/her hands free to inspect rather than having to use them to enter data. Another possible application might involve an inventory operation. If bar code scanning were the primary technology being used for the inventory operation, and a bar code label were found to be missing from an item, the conventional technique would be to key in the item's serial number or description. A voice system would be quicker and more accurate than a keyed input and could therefore be used as a robust backup to the bar code data entry system.

The Industry

There are three primary US companies which manufacture portable speech recognition systems. They are: Vocollect, Verbex, and Voice Connexion. Approximate costs, and brief summaries of the salient features of these companies' systems are provided below.

Vocollect:

Location:	Pittsburgh, PA
Telephone:	412-829-8145
Contact:	Elmer Harkema
Hardware:	$6500/unit (belt-worn unit + battery pack)
Software:	$6000/site

Product Description: Portable system comprised of: a headset for speaking and listening; a belt-worn CPU weighing slightly more than one pound; software; belt-worn battery pack weighing about two pounds

Major Applications: Shipping/receiving; inventory management; defect inspections, maintenance inspections

Key Customers: GM, GE, IBM, US Army, Westinghouse

Verbex:

Location:	New Jersey
Telephone:	908-225-5225
Contact	Bill Nicolosi (x3020)
Hardware:	$3000/unit (belt-worn unit + battery pack)
Software:	$139/unit ("Listen For Windows")

Product Description: Portable system comprised of: a headset for speaking and listening; a belt-worn CPU weighing slightly more than one pound; software; belt-worn battery pack weighing about two pounds

Major Applications: Shipping/receiving; inventory management; defect inspections, maintenance inspections

Key Customers: Not Available

Voice Connexion

Location:	Irvine, California
Phone:	714-261-2366
Contact:	Shirley Dworak (VP Sales/Marketing)
Hardware:	$1495 (belt-worn unit plus headset)
	$79 (battery pack)

Product Description: Portable system comprised of: a headset for speaking and listening; a belt-worn CPU weighing about 1/2 pound; battery pack weighing about three pounds, software

Major Applications: Shipping/receiving; inventory management; defect inspections, maintenance inspections

Major Customers: AT&T, Lockheed, Boeing, Pepsi Cola, U.S. Army/TACOM, Telxon

Biometric Identification Technology

Background

Biometric identification is a broad category of technologies which provide precise confirmation of an individual's identity through the use of that individual's own physiological or behavioral characteristics. A physiological characterisitic is a relatively stable physical characteristic such as a fingerprint, retinal scan, hand geometry, or facial features. Behavioral characteristics are influenced by the individual's personality. These include voice print, signature and keystroke. Biometric technology is beginning to be more widely used for automated access control, as well as to confirm an individual's actual presence at a specific location at a given date and time.

Most biometric identification systems use a card or PIN for initial identification. In this way the system does not search through the entire database for a potential match. The system goes directly to the stored template corresponding to the card or PIN. The biometric measurement is used to verify that the individual holding the card or entering the PIN is the legitimate owner of the card or PIN. The cost for these systems includes the hardware needed to read the card, enter a PIN, etc. If the biometric measurement is stored in the card itself, then the comparison can be done off-line at the entry point, without having to do back to a central system.

Some common applications of biometric verification technology today include:

- physical access control
- computer security - access to secure files and networks
- automated financial transaction verification
- welfare fraud protection
- field use in law enforcement
- immigration status when entering into a country

Future applications include: "key" replacements for home or vehicle access, replacement of physical cards for credit card purchases, personalized, intelligent switches for devices (e.g., guns), electronic signatures for transfer of custodial property such as legal evidence, etc. The average cost of biometric verifiers is about $2000 per access point. Voice and signature verifiers can be purchased for under $1000, and highly secure hand geometry and fingerprint devices are available for $1,200 - $5,000. Prices are expected to continue dropping, making biomertic verification affordable in many applications.

The Technologies

Fingerprint

The most widely used biometric technique is fingerprint identification. Since fingerprints have been used in forensic (criminal science) applications for over a hundred years, there is a wealth of information concerning the uniqueness of fingerprint patterns. Most fingerprint technology systems rely on classifying the ridge and valley patterns of the fingerprint into specific "minutiae." This minutiae is then characterized and stored as an individual's fingerprint template. Depending upon the methodology of the device and the security level required, storing a fingerprint template requires approximately 1000 bytes. This is one of the largest biometric templates.

Fingerprint verifiers are very reliable. The false acceptance rate is less than one in a million. Machines do reject approxximately 3% of authorized users. Considerations include: not always placing the finger in the same position, a healing wound on the finger, quality of image capture, and quality of the matching algorithm.

Retinal Scan

Retinal scan technology employs optical technology to map the capillary pattern of the retina of the eye. This technology produces a unique print similar to fingerprint. The retinal pattern template only requires about 35 bytes. The primary application for this technology has been in high-security access control. Retinal scans are extremely reliable. They have a 0% false acceptance rate, and they rarely reject an authorized user.

Hand Geometry

Hand geometry systems employ optical systems to "map" key geometric features of the topography of a hand to verify an individual's identity. The systems have been used for physical access control and recently by the US Immigration and Naturalization Service to verify the identity of international travelers who enter the US on a frequent basis. These systems have a high rate of acceptance amongst users, as they do not have the "criminal" connotations associated with fingerprints or the fear of injury associated with retinal scans. The hand geometry template requires only 10 bytes, the smallest in the industry.

Facial Features

Facial feature recognition is the fastest growing area in the biometric industry. The rapid rise in multimedia technology is stimulating development of various video technologies. Given the already frequent use of survellience camaras in security applications, this technology is the next logical step to augment these systems. Facial feature verification systems are expected to have a high rate of acceptance amongst users, as most people are used to being phtographed, and it is the manner in which people most recognize one another.

Voice Verification

Voice verification can combine password protection and biometric verification in one process. This means that a separate keypad is not required to enter the PIN or password, as the individual speaks the PIN or password to gain system access. Verification is accomplished by comparing the spoken PIN or password to the individual's digitally stored voice-print. Voice is a very convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access. A telephone purchase which uses a credit card number could also use a voice system to confirm that the individual making the purchase is the legitimate owner of that credit card. Voice systems are gaining in popularity due to the increase in telephonic business, and because they have a high rate of acceptance amongst users.

Signature

The signature has been a common form of authentication for many years. An important feature in *automated* signature identification systems is the ability to differentiate between aspects of the signature that are habitual (consistent), and aspects that change nearly every time the person signs their name. Though these systems have been slower to catch on, it is generally agreed that these systems will become more popular in the future. There are over 100 patents issued in this area.

Keystroke

Perhaps one of the most innovative and unusual biometric technologies is keystroke verification, also called typing rthythms. This method of biometric verification analyses the way a person types by monitoring their keyboard input 1000 times per second. Studies conducted by the National Sciences Foundation and the National Institue of Standards and Technology have established that typing patterns are unique. There are advantages to using keystoke verification in computer access applications. Not only is it unnecessary for the user to go through some special process to enroll in the system, the verificaton occurs seemlessly while they are doing their job. While these systems are still in development, current research is expected to result in very successful commercial systems.

Biometric Companies

Fingerprint

Digital Biometrics, Inc. 5600 Rowland Road, Suite 205 Minnetonka MN 55343-8956 (612) 932-0888	Cogent Systems, Inc. 3001-A West Mission Road Alhambra CA 91803 (818) 300-8828	Comparator Systems Corp. 4350 Von Karman Ave, Suite 180 Newport Beach CA 92660 (714) 851-4300
Fingermatrix Inc. 145 Palisade Street Dobbs Ferry NY 10522 (914) 693-1050	Identicator Technology 851 Traeger Avenue, Suite 310 San Bruno CA, 94066 (415) 873-8650	Identix, Inc. 510 North Pastoria Avenue Sunnyvale CA 94086 (408) 739-2000

Hand Geometry	**Retinal Scan**	**Signature**
Recognition Systems, Inc. 62 South San Tomas Aquino Rd Campbell CA 95959 (408) 364-6960	EyeDentify, Inc. 10473 Old Hammond Hwy. Baton Rouge LA 70816 (504) 927-4290	CheckMate Electronics 1011 Mansell Road, Suite C Roswell GA 30076 (404) 594-6000
PIDEAC 225 Park Meadows Dr. Box 561 Yellow Springs OH 45397 (513) 767-7425	IriScan, Inc. 133-Q Gaither Drive Mt. Laural NJ 08054 (609) 234-7977	Communication Intelligence Corp. 275 Shoreline Drive, Fifth Floor Redwood Shores CA 94065 (415) 802-7888

Facial Features	**Voice Verification**	
NeuroMetric Vision Systems, Inc. 2655 S. Le Jeune Rd. Coral Gables FL 33134 (305) 447-8919	Bellcore 445 South Street, MRE-2A269 Morristown NJ 07960 (201) 829-4133	Texas Instruments, Inc. 12501 Research Blvd, MS 2243 Austin TX 78714 (512) 250-6542
	Voice Sciences Corporation 750 Hammond Drive, Building 7 Atlanta GA 30328 (404) 255-8370	Voice Strategies 4555 Corporate Drive, Suite 306 Troy MI 48098 (810) 641-8600